We Claim:

1. A video game system for executing a video game program and generating game play graphics for display on a user's display comprising:

a game processing system for executing a video game program and generating game play graphics on a user's display;

communications circuitry, coupled in use to said game processing system and to a user's communications network, for linking said game processing system to a server;

a writeable mass storage device having a plurality of groups of storage locations and coupled in use to said game processing system for storing at least graphics data loaded therein;

a mass storage device controller for controlling access to said plurality of groups of storage locations in said writeable mass storage device, said mass storage device controller including cryptographic processing circuitry for performing cryptographic operations on information communicated between said video game system and said server.

2. A video game system according to claim 1, wherein said mass storage device controller is operable to generate a game request

packet and transmit the game request packet in encrypted form to said server.

3. A video game system according to claim 1, wherein said cryptographic processing circuitry performs encryption processing and wherein said mass storage device has an associated unique ID which is associated with at least one encryption key that is used during encryption processing.

4. A video game system according to claim 1, wherein said mass storage device controller includes a digital processor coupled to said cryptographic processing circuitry and to said mass storage device.

5. A video game system according to claim 4, further including a random access memory coupled to said digital processor and a read-only memory coupled to said digital processor.

6. A video game system according to claim 1, wherein each group of storage locations is a partition, wherein said mass storage device is operable to store a partition table defining the mass storage device partitions which are accessible to a game program and wherein said digital processor is operable to maintain said partition table.

7. A video game system according to claim 6, wherein said partition table associates a game program with a read-only partition for storing encrypted game program instructions.

8. A video game system according to claim 1, wherein said mass storage device controller includes a digital processor and said cryptographic processing circuitry is coupled to said digital processor for decrypting encrypted game program instructions accessed from said mass storage device.

9. A video game system according to claim 6, wherein an executing game program has access to a plurality of private partitions defined by said partition table.

10. A video game system according to claim 1, wherein said mass storage device controller includes a digital processor and said cryptographic processing circuitry is coupled to said digital processor and to said mass storage device, wherein said cryptographic processing circuitry is operable to compute a hash value for ensuring that information transmitted between said server and said mass storage device controller has not been corrupted.

11. A video game system according to claim 10, wherein the data on which a hash value is to be computed is used as a key during the hash computation.

12. A video game system according to claim 1, wherein said mass storage device controller is operable to detect security faults and to generate random data in response to its detection of a security fault.

13. A video game system according to claim 1, wherein each group of storage locations is a partition and wherein said mass storage device includes a plurality of partitions which are shared by a plurality of game programs.

14. A video game system according to claim 1, wherein said mass storage device stores unique data loaded during the manufacturing process which is used during cryptographic operations.

15. A video game system according to claim 14, wherein said unique data includes at least one private encryption key.

16. A video game system according to claim 14, wherein said unique data includes a mass storage device identifier uniquely identifying a particular mass storage device.

17. A video game system according to claim 1, wherein an executing video game is only permitted to access predetermined groups of storage locations of said mass storage device under the control of said mass storage device controller.

18. A video game system according to claim 1, wherein said server is operable to download a video game in response to an encrypted game request uniquely identifying the requesting mass storage device.

19. A video game system according to claim 1, wherein said mass storage device controller is operable to place said mass storage device in a write-only state.

20. A video game system according to claim 19, wherein said write-only state is set during application downloading operations from said server to said mass storage device.

21. A video game system according to claim 20, wherein said write-only state is cleared at the completion of a successful download operation from said server to said mass storage device.

22. A video game system according to claim 1, wherein said mass storage device controller includes a random access memory and wherein said mass storage device controller executes a security

program, the location of which is distributed between said mass storage device and said random access memory.

23. A video game system according to claim 1, wherein said server includes a master server for receiving at least one encryption key from a mass storage device controller and for performing cryptographic operations therewith and an electronic commerce server associated with a user's Internet service provider.

24. A video game system according to claim 1, wherein messages are transmitted overtime between said server and said mass storage device controller, said messages including a message counter field which is incremented each time a message is sent.

25. Information processing apparatus for executing an applications program and for generating graphics for display on a user's display comprising:

an information processing system for executing an applications program and generating graphics on a user's display;

communications circuitry, coupled in use to said information processing system and to a user's communications network, for linking said information processing system to a server;

a writeable mass storage device having a plurality of groups of storage locations and coupled in use to said information processing system for storing at least graphics data loaded therein;

a mass storage device controller for controlling access by said applications program to said plurality of groups of storage locations in said writeable mass storage device, said mass storage device controller including cryptographic processing circuitry for performing cryptographic operations on information communicated between said information processing system and said server.

26. An information processing apparatus according to claim 25, wherein said applications program is a video game program and said mass storage device controller is operable to generate a game request packet and transmit the game request packet in encrypted form to said server.

27. An information processing apparatus according to claim 25, wherein said cryptographic processing circuitry performs encryption processing and wherein said mass storage device has an associated unique ID which is associated with at least one encryption key that is used during encryption processing.

28. An information processing apparatus according to claim 25, wherein said mass storage device controller includes a digital processor coupled to said cryptographic processing circuitry and to said mass storage device.

29. An information processing apparatus according to claim 28, further including a random access memory coupled to said digital processor and a read-only memory coupled to said digital processor.

30. An information processing apparatus according to claim 25, wherein each group of storage locations is a partition and wherein said mass storage device is operable to store a partition table defining the mass storage device partitions which are accessible to an applications program and wherein said digital processor is operable to maintain said partition table.

31. An information processing apparatus according to claim 30, wherein said partition table associates an applications program with a read-only partition for storing encrypted application program instructions.

32. An information processing apparatus according to claim 25, wherein said mass storage device controller includes a digital processor and wherein said cryptographic processing circuitry is

coupled to said digital processor for decrypting encrypted applications program instructions accessed from said mass storage device.

33. An information processing apparatus according to claim 30, wherein an executing applications program has access to a plurality of private partitions defined by said partition table.

34. An information processing apparatus according to claim 25, wherein said mass storage device controller includes a digital processor and wherein said cryptographic processing circuitry is coupled to said digital processor and to said mass storage device, wherein said cryptographic processing circuitry is operable to compute a hash value for ensuring that information transmitted between said server and said mass storage device controller has not been corrupted.

35. An information processing apparatus according to claim 34, wherein the data on which a hash value is to be computed is used as a key during the hash computation.

36. An information processing apparatus according to claim 25, wherein said mass storage device controller is operable to detect

security faults and to generate random data in response to its detection of a security fault.

37. An information processing apparatus according to claim 25, wherein each group of storage locations is a partition and wherein said mass storage device includes a plurality of partitions which are shared by a plurality of applications programs.

38. An information processing apparatus according to claim 25, wherein said mass storage device stores unique data loaded during the manufacturing process which is used during cryptographic operations.

39. An information processing apparatus according to claim 38, wherein said unique data includes at least one private encryption key.

40. An information processing apparatus according to claim 38, wherein said unique data includes a mass storage device identifier uniquely identifying a particular mass storage device.

41. An information processing apparatus according to claim 25, wherein each group of storage locations is a partition and wherein an executing applications program is only permitted to access

predetermined partitions of said mass storage device under the control of said mass storage device controller.

42. An information processing apparatus according to claim 25, wherein said server is operable to download an applications program in response to an encrypted applications program request uniquely identifying the requesting mass storage device.

43. An information processing apparatus according to claim 25, wherein said mass storage device controller is operable to place said mass storage device in a write-only state.

44. An information processing apparatus according to claim 43, wherein said write-only state is set during application downloading operations from said server to said mass storage device.

45. An information processing apparatus according to claim 44, wherein said write-only state is cleared at the completion of a successful download operation from said server to said mass storage device.

46. An information processing apparatus according to claim 25, wherein said mass storage device controller includes a random access memory and wherein said mass storage device controller

executes a security program, the location of which is distributed between said mass storage device and said random access memory.

47. An information processing apparatus according to claim 25, wherein said server includes a master server for receiving at least one encryption key from a mass storage device controller and for performing cryptographic operations therewith and an electronic commerce server associated with a user's Internet service provider.

48. An information processing apparatus according to claim 25, wherein messages are continuously transmitted between said server and said mass storage device controller, said messages including a message counter field which is incremented each time a message is sent.